CLAIMS

What is claimed is:

1. A method for providing access and tracking the access of a non-registered individual at a secure point of entry to a secure environment comprising:

   a. establishing the secure environment by an owner, wherein the secure environment comprises the secure point of entry, and wherein the secure point of entry is assigned an environment Risk Factor;

   b. requesting entry into the secured environment at the secure point of entry by an individual, wherein the individual comprises identification information, and wherein the identification information comprises an individual identifier;

   c. sending the individual identifier to an authentication database established by a third party, wherein the authentication database comprises records for registered individuals;

   d. receiving a response from the authentication database, wherein the response states that the individual is a non-registered individual;

   e. asking the non-registered individual a plurality of questions, wherein the non-registered individual answers the plurality of questions creating a profile, wherein an individual Risk Factor is assigned to the individual based upon the profile;

   f. registering the non-registered individual with the individual Risk Factor on the authentication database by creating a record comprising the individual identifier and the individual Risk Factor;

   g. making a comparison between the individual Risk Factor and the environment Risk Factor;

   h. making a determination whether the individual is allowed entry into the secured environment based upon the comparison; and

i. adding the determination to the record of the individual in the authentication database.

2. The method of claim 1, wherein the secure environment is selected from the group consisting of a bank, a computer program, an airport, a train, an airplane, a truck, a military vehicle, a car, a building, offices, an open space, a specified area, a computer, a border of a country, an internal country checkpoint, and combinations thereof.

3. The method of claim 1, wherein the step of requesting entry into the secured environment at the secure point of entry by an individual is performed by a member of the group consisting of a fingerprint reader, a numerical code, a voice pattern recognition reader, a retinal scanner, a telemetry card reader, a smart card reader, other biometric readers, and combinations thereof.

4. The method of claim 1, wherein the steps of requesting entry into the secured environment at the secure point of entry is performed by a secondary party, wherein the secondary party is selected from the group consisting of a secretary, a clerk, an employee, a security guard, a contract worker, and combinations thereof.

5. The method of claim 1, wherein the steps of sending the individual identifier additional information and receiving a response from the authentication database is transmitted by standard voice and data transmission.

6. The method of claim 1, wherein the authentication database is linked to a secondary database, wherein secondary database is selected from the group consisting of Interpol database, United States Border Patrol database, US police database, US FBI database, US CIA database, state agency fingerprint databases, and other state authentication database, immigration databases, and combinations thereof.

7. The method of claim 6, wherein the response from the authentication database further comprises information obtained from the secondary database.

8. The method of claim 1, further comprising the step of holding the individual for questioning when the individual Risk Factor is high, wherein the questioning is performed by a governmental authority or the owner.

9. The method of claim 1, wherein the identification information is selected from the group consisting of fingerprint, a numerical code, a voice sample, an eye scan, individual's name, individual's pictures, individual's demographics, and combinations thereof.

10. The method of claim 1, wherein the step of asking the non-registered individual the plurality of questions comprises asking questions pertaining to individual's immigration; individual's police records; individual's arrests; individual's occupation; individual's possessions; individual's parole status; individual's dates of prior admissions to the secure environment; individual's dates of prior denials to the secure environment; individual's prior seizures of items prohibited in the secure environment; individual's name, individual's address, individual's nationality, individual's height, individual's weight, individual's social security number, individual's passport number, individual's government identification type, individual's government identification number, individual's credit card number, individual's finger print, individual's digital photo, individual's age, and combination thereof.

11. The method of claim 1, further comprising the step of presenting the individual with a smart card after registering the individual in the authentication database, wherein the smart cart comprises the individual identifier.

12. The method of claim 11, wherein the smart card is only usable by the individual with a proper biometric key.

13. A method for providing access and tracking of the access of a registered individual at a secure point of entry to a secure environment comprising:

a. establishing the secure environment by an owner, wherein the secure environment comprises the secure point of entry, and wherein the secure point of entry is assigned an environment Risk Factor;

b. requesting entry into the secured environment at the secure point of entry by an individual, wherein the individual comprises identification information, and wherein the identification information comprises an individual identifier;

c. sending the individual identifier to an authentication database established by a third party, wherein the authentication database comprise records for registered individuals;

d. receiving a response from the authentication database, wherein the response states that the individual is a registered individual, and wherein the response comprises the individual Risk Factor assigned to the individual;

e. making a comparison between the individual Risk Factor and environment Risk Factor;

f. making a determination whether the individual is allowed entry into the secured environment based upon the comparison; and

g. adding the determination to the record of the registered individual in the authentication database.

14. The method of claim 13, further comprising the step of asking the individual a plurality of questions, wherein the individual answers the plurality of questions creating a profile, wherein the individual Risk Factor is modified based upon the profile.

15. The method of claim 14, further comprising the step of holding the individual for questioning when the individual Risk Factor is high, wherein the questioning is performed by a governmental authority or the owner.

16. The method of claim 14, wherein the step of asking the non-registered individual the plurality of questions comprises asking questions pertaining to individual's immigration; individual's police records; individual's arrests; individual's occupation; individual's possessions; individual's parole status; individual's dates of prior admissions to the secure environment; individual's dates of prior denials to the secure environment; individual's prior seizures of items prohibited in the secure environment; individual's

name, individual's address, individual's nationality, individual's height, individual's weight, individual's social security number, individual's passport number, individual's government identification type, individual's government identification number, individual's credit card number, individual's finger print, individual's digital photo, individual's age, and combination thereof.

17. The method of claim 1, wherein the steps of sending the individual identifier additional information and receiving a response from the authentication database is transmitted by standard voice and data transmission.

18. The method of claim 1, wherein the authentication database is linked to a secondary database, wherein secondary database is selected from the group consisting of Interpol database, United States Border Patrol database, US police database, US FBI database, US CIA database, state agency fingerprint databases, and other state authentication database, immigration databases, and combinations thereof.

19. The method of claim 18, wherein the response from the authentication database further comprises information obtained from the secondary database.

20. The method of claim 1, further comprising the step of holding the individual for questioning when the individual Risk Factor is high, wherein the questioning is performed by a governmental authority or the owner.

21. The method of claim 1, wherein the identification information is selected from the group consisting of fingerprint, a numerical code, a voice sample, an eye scan, individual's name, individual's pictures, individual's demographics, and combinations thereof.

22. The method of claim 13, further comprising the step of presenting a smart card by the individual requesting entry into the secured environment at the secure point of entry, wherein the smart comprises information specific to the individual.

23. The method of claim 14, wherein the smart card is only usable by the individual with a proper biometric key.